Access Control and Authenticator Management

Aligned with NIST SP 800-53 Rev. 5

Company Name: SecurePath Tech Solutions, Inc.

Policy Title: Access Control and Authenticator Management Policy

Policy ID: ISP-AC-001

Effective Date: 2025-01-01

Revision: 1.0

Policy Owner: Chief Information Security Officer (CISO)

Classification: Internal Use Only

1. Purpose

The purpose of this policy is to establish guidelines for access control and authenticator management in accordance with NIST SP 800-53 Rev. 5. This policy ensures that access to information systems is limited to authorized users and devices, thereby protecting the confidentiality, integrity, and availability of organizational information.

2. Scope

This policy applies to all employees, contractors, and third-party users who have access to information systems and data owned or managed by the organization.

3. Policy Statements

3.1 Access Control (AC)

- Access to systems must be based on the principles of least privilege and separation of duties
- Access authorizations must be reviewed every 90 days
- Role-based access controls (RBAC) must be implemented where feasible

3.2 Account Management (AC-2)

- All user accounts must be uniquely identifiable
- Accounts must be deactivated after 30 days of inactivity unless otherwise approved
- Temporary accounts must have defined expiration dates

3.3 Authenticator Management (IA-5)

- Passwords must meet complexity requirements and be changed every 90 days
- Multi-Factor Authentication (MFA) must be used for privileged and remote access
- Default passwords must be changed before initial use

4. Responsibilities

- The Information Security Officer is responsible for policy enforcement and review
- System administrators are responsible for configuring access controls and managing authenticators
- Users are responsible for protecting their credentials and reporting any suspicious activities

5. Compliance

Violations of this policy may result in disciplinary action, up to and including termination of access or employment. The organization reserves the right to audit compliance with this policy.

6. Review and Updates

This policy shall be reviewed annually and updated as necessary to reflect changes in organizational needs or regulatory requirements.